EXHIBIT C-13
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 6 ('661 Patent)	**U.S. 5,181,243 to Saltwick et al. ("Saltwick")**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:5-7 – "This invention relates to communications systems, and more particularly to security protection arrangements therefor." 1:8-19 – "The use of the public telephone system for computer communications and other data services is widespread. Services which are provided involve access to bank accounts, credit limit reporting, credit card transactions, and order entry functions. Communications are typically accomplished by encoding data to be transmitted as data signals. Examples of encoding are frequency shift keying (FSK), phase shift keying (PSK), and other forms of modulation using modems. Among the more popular forms of transmission are dual tone multi-frequency data (DTMF), commonly called Touchtone, and multi-frequency (MF) data encoding." 1:29-33 – "It is the primary object of this invention to provide a security system which makes it difficult or impossible to compromise security by eavesdropping on the telephone connection during the transmission of sensitive data." 2:3-9 – "In order to mask the transmission of DTMF digits, a masking signal consisting of at least two row tones or two column tones can be used. Thus, no matter what row and column tones characterize a transmitted digit, an eavesdropper would detect at least three tones on the transmission line with no way to determine which two constitute the actual DTMF digit." 4:2-13 – "Signal processing is most conveniently implemented by using standard digital signal processing integrated circuits, such as the Texas Instruments TMS320C25 integrated circuit. There are standard echo cancellation and sidetone cancellation algorithms used in the art, and these types of algorithm can be used in the more sophisticated embodiments of the invention shown in FIGS. 6 and 7. It is to be understood, however, that analog signal processing techniques can also be used. In any event, the embodiment of FIG. 5 requires relatively unsophisticated signal processing." Claim 1 – "In a communication system wherein information signals are generated by a sending device and communicated to a receiving device, said information signals being dual tone multi-frequency digits, each digit of which is represented by one of four row

	frequencies and one of four column frequencies, apparatus for securing said information signals comprising: means for superimposing a masking signal on said information signals to generate composite communicated signals, rendering interceptions of said communicated signals unintelligible, said masking signal consisting of at least two row frequencies or at least two column frequencies; and means for extracting said information signal from said composite communicated signals."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:35-38 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector." 2:35-43 – "The sending device 10 may be a telephone instrument capable of transmitting DTMF signals, or it may be a more sophisticated automated device such as a credit card transaction terminal. FIG. 8 depicts a typical DTMF keypad, along with the row and column frequency assignments which are in common use. The receiving device 20 in FIG. 1 is typically a computer, with a front end processor often connecting the computer to the telephone line. As is well known in the art, the path may be established over trunk lines between two or more central offices 14, 16. There may also be other intervening facilities, such as PBXs 12, 18."
(b) a source of unpredictable information;	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase." 3:31-33 – "As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30." 6:6-16 – "Therefore, to keep the eavesdropping devices confused as to what the masking signal actually is, the masking signal may be varied over time in frequency, amplitude and/or phase. A random pattern is

	best for the receiving end to transmit. A random pattern is difficult for eavesdropping detectors to predict and therefore they are more likely to lose the information signal. For DTMF coding, masking signal generator 33 preferably varies the frequency between row and column frequencies, out-of-band frequencies and other in-band frequencies."
(c) a processor:	2:41-43 – "The receiving device 20 in FIG. 1 is typically a computer, with a front end processor often connecting the computer to the telephone line. As is well known in the art, the path may be established over trunk lines between two or more central offices 14, 16. There may also be other intervening facilities, such as PBXs 12, 18."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	2:34-47 – "FIG. 1 depicts a typical data communications path over the switched public telephone network. The sending device 10 may be a telephone instrument capable of transmitting DTMF signals, or it may be a more sophisticated automated device such as a credit card transaction terminal. FIG. 8 depicts a typical DTMF keypad, along with the row and column frequency assignments which are in common use. The receiving device 20 in FIG. 1 is typically a computer, with a front end processor often connecting the computer to the telephone line. As is well known in the art, the path may be established over trunk lines between two or more central offices 14, 16. There may also be other intervening facilities, such as PBXs 12, 18." Figure 1.
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	5:44-53 – "The concept is also applicable to the use of column frequencies as masking signals. It has been found experimentally that two row frequencies and one column frequency provide the best confusion to DTMF detectors. This is primarily due to more energy at invalid frequencies being present at the decoder, thus providing greater confusion for eavesdropping detectors. (Some frequencies other than row and column frequencies have been found effective as masking signals. However, they have not thus far provided consistent masking for eavesdropping devices.)" 6:6-16 – "Therefore, to keep the eavesdropping devices confused as to what the masking signal actually is, the masking signal may be varied over time in frequency, amplitude and/or phase. A random pattern is best for the receiving end to transmit. A random pattern is difficult for eavesdropping detectors to predict and therefore they are more likely to lose the information signal. For DTMF coding, masking signal generator 33 preferably varies the frequency between row and column frequencies, out-of-band frequencies and other in-band frequencies."
(d) an output interface	3:18-31 -- "The most elementary form of the invention is shown in

for outputting said cryptographically processed quantity to a recipient thereof.	FIG. 4. In data communications a hybrid 24 is sometimes used anyway. Receive channel 28 is shown extended to a receiving device, which is typically a DTMF detector at the data processing site. Very often it is necessary to transmit signals to the sending device, typically automated voice signals under the control of the data processor. For this purpose a transmit channel 30 is utilized, and hybrid 24 serves to couple transmitted signals to telephone line 26, and to couple signals on the telephone line to the receiving device over channel 28." 3:31-38 – "The hybrid serves to attenuate the transmitted signals on channel 30 such that they appear at a much lower level on the receive channel 28. As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30. Voice or even data signals may also be applied on channel 30, but the significant thing about masking signal generator 33 is that it applies a masking signal on channel 30 at the time that the sending device 10 of FIG. 1 transmits sensitive data in the opposite direction to the receiving device."

Claim 11 ('661 Patent)	**U.S. 5,181,243 to Saltwick**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:5-7 – "This invention relates to communications systems, and more particularly to security protection arrangements therefor." 1:8-19 – "The use of the public telephone system for computer communications and other data services is widespread. Services which are provided involve access to bank accounts, credit limit reporting, credit card transactions, and order entry functions. Communications are typically accomplished by encoding data to be transmitted as data signals. Examples of encoding are frequency shift keying (FSK), phase shift keying (PSK), and other forms of modulation using modems. Among the more popular forms of transmission are dual tone multi-frequency data (DTMF), commonly called Touchtone, and multi-frequency (MF) data encoding." 1:29-33 – "It is the primary object of this invention to provide a security system which makes it difficult or impossible to compromise security by eavesdropping on the telephone connection during the transmission of sensitive data." 2:3-9 – "In order to mask the transmission of DTMF digits, a masking signal consisting of at least two row tones or two column tones can be used. Thus, no matter what row and column tones characterize a transmitted digit, an eavesdropper would detect at least three tones on the transmission line with no way to determine which two constitute

	the actual DTMF digit." Claim 1 – "In a communication system wherein information signals are generated by a sending device and communicated to a receiving device, said information signals being dual tone multi-frequency digits, each digit of which is represented by one of four row frequencies and one of four column frequencies, apparatus for securing said information signals comprising: means for superimposing a masking signal on said information signals to generate composite communicated signals, rendering interceptions of said communicated signals unintelligible, said masking signal consisting of at least two row frequencies or at least two column frequencies; and means for extracting said information signal from said composite communicated signals."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:35-38 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector." 2:35-43 – "The sending device 10 may be a telephone instrument capable of transmitting DTMF signals, or it may be a more sophisticated automated device such as a credit card transaction terminal. FIG. 8 depicts a typical DTMF keypad, along with the row and column frequency assignments which are in common use. The receiving device 20 in FIG. 1 is typically a computer, with a front end processor often connecting the computer to the telephone line. As is well known in the art, the path may be established over trunk lines between two or more central offices 14, 16. There may also be other intervening facilities, such as PBXs 12, 18."
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase."

	5:38-53 – "Therefore, if two row tones are used as the masking signal, all digits will be blocked from detection. It has been found that the row 1 and row 4 frequencies are the best choices; this combination produces uniform blocking for all digits. The concept is also applicable to the use of column frequencies as masking signals. It has been found experimentally that two row frequencies and one column frequency provide the best confusion to DTMF detectors. This is primarily due to more energy at invalid frequencies being present at the decoder, thus providing greater confusion for eavesdropping detectors. (Some frequencies other than row and column frequencies have been found effective as masking signals. However, they have not thus far provided consistent masking for eavesdropping devices.)"
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	2:34-47 – "FIG. 1 depicts a typical data communications path over the switched public telephone network. The sending device 10 may be a telephone instrument capable of transmitting DTMF signals, or it may be a more sophisticated automated device such as a credit card transaction terminal. FIG. 8 depicts a typical DTMF keypad, along with the row and column frequency assignments which are in common use. The receiving device 20 in FIG. 1 is typically a computer, with a front end processor often connecting the computer to the telephone line. As is well known in the art, the path may be established over trunk lines between two or more central offices 14, 16. There may also be other intervening facilities, such as PBXs 12, 18." Figure 1.
(d) a noise production system for introducing noise into said measurement of said power consumption.	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase." 3:31-33 – "As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30." 6:6-16 – "Therefore, to keep the eavesdropping devices confused as to what the masking signal actually is, the masking signal may be varied

	over time in frequency, amplitude and/or phase. A random pattern is best for the receiving end to transmit. A random pattern is difficult for eavesdropping detectors to predict and therefore they are more likely to lose the information signal. For DTMF coding, masking signal generator 33 preferably varies the frequency between row and column frequencies, out-of-band frequencies and other in-band frequencies." 5:38-53 – "Therefore, if two row tones are used as the masking signal, all digits will be blocked from detection. It has been found that the row 1 and row 4 frequencies are the best choices; this combination produces uniform blocking for all digits. The concept is also applicable to the use of column frequencies as masking signals. It has been found experimentally that two row frequencies and one column frequency provide the best confusion to DTMF detectors. This is primarily due to more energy at invalid frequencies being present at the decoder, thus providing greater confusion for eavesdropping detectors. (Some frequencies other than row and column frequencies have been found effective as masking signals. However, they have not thus far provided consistent masking for eavesdropping devices.)"

Claim 12 ('661 Patent)	**U.S. 5,181,243 to Saltwick**
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase." 3:31-33 – "As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30." 6:6-16 – "Therefore, to keep the eavesdropping devices confused as to what the masking signal actually is, the masking signal may be varied over time in frequency, amplitude and/or phase. A random pattern is best for the receiving end to transmit. A random pattern is difficult for eavesdropping detectors to predict and therefore they are

	more likely to lose the information signal. For DTMF coding, masking signal generator 33 preferably varies the frequency between row and column frequencies, out-of-band frequencies and other in-band frequencies."
(b) a noise processing module for improving the random characteristic of said initial noise; and	3:38-47 – "The masking signal is shown symbolically in FIG. 4, and it appears together with the information signal transmitted in the opposite direction on line 26. The function of hybrid 24 is to reduce the amplitude of the masking signal relative to that of the information signal on receive channel 28. It is in this way that the receiving device can discriminate between the information and masking signals, while an unauthorized tapping of line 26 will not result in intelligible interception of the information signal." Figure 4.
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	5:46-53 – "This is primarily due to more energy at invalid frequencies being present at the decoder, thus providing greater confusion for eavesdropping detectors. (Some frequencies other than row and column frequencies have been found effective as masking signals. However, they have not thus far provided consistent masking for eavesdropping devices.)"

Claim 29 ('661 Patent)	**U.S. 5,181,243 to Saltwick**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:5-7 – "This invention relates to communications systems, and more particularly to security protection arrangements therefor." 1:8-19 – "The use of the public telephone system for computer communications and other data services is widespread. Services which are provided involve access to bank accounts, credit limit reporting, credit card transactions, and order entry functions. Communications are typically accomplished by encoding data to be transmitted as data signals. Examples of encoding are frequency shift keying (FSK), phase shift keying (PSK), and other forms of modulation using modems. Among the more popular forms of transmission are dual tone multi-frequency data (DTMF), commonly called Touchtone, and multi-frequency (MF) data encoding." 1:29-33 – "It is the primary object of this invention to provide a security system which makes it difficult or impossible to compromise security by eavesdropping on the telephone connection during the transmission of sensitive data." 2:3-9 – "In order to mask the transmission of DTMF digits, a masking

	signal consisting of at least two row tones or two column tones can be used. Thus, no matter what row and column tones characterize a transmitted digit, an eavesdropper would detect at least three tones on the transmission line with no way to determine which two constitute the actual DTMF digit." Claim 1 – "In a communication system wherein information signals are generated by a sending device and communicated to a receiving device, said information signals being dual tone multi-frequency digits, each digit of which is represented by one of four row frequencies and one of four column frequencies, apparatus for securing said information signals comprising: means for superimposing a masking signal on said information signals to generate composite communicated signals, rendering interceptions of said communicated signals unintelligible, said masking signal consisting of at least two row frequencies or at least two column frequencies; and means for extracting said information signal from said composite communicated signals."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase." 5:38-53 – "Therefore, if two row tones are used as the masking signal, all digits will be blocked from detection. It has been found that the row 1 and row 4 frequencies are the best choices; this combination produces uniform blocking for all digits. The concept is also applicable to the use of column frequencies as masking signals. It has been found experimentally that two row frequencies and one column frequency provide the best confusion to DTMF detectors. This is primarily due to more energy at invalid frequencies being present at the decoder, thus providing greater confusion for eavesdropping detectors. (Some frequencies other than row and column frequencies have been found effective as masking signals. However, they have not thus far provided consistent masking for

	eavesdropping devices.)"
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:35-38 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector." 2:35-43 – "The sending device 10 may be a telephone instrument capable of transmitting DTMF signals, or it may be a more sophisticated automated device such as a credit card transaction terminal. FIG. 8 depicts a typical DTMF keypad, along with the row and column frequency assignments which are in common use. The receiving device 20 in FIG. 1 is typically a computer, with a front end processor often connecting the computer to the telephone line. As is well known in the art, the path may be established over trunk lines between two or more central offices 14, 16. There may also be other intervening facilities, such as PBXs 12, 18."
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase." 3:31-33 – "As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30." 6:6-16 – "Therefore, to keep the eavesdropping devices confused as to what the masking signal actually is, the masking signal may be varied over time in frequency, amplitude and/or phase. A random pattern is best for the receiving end to transmit. A random pattern is difficult for eavesdropping detectors to predict and therefore they are more likely to lose the information signal. For DTMF coding, masking signal generator 33 preferably varies the frequency between row and column frequencies, out-of-band frequencies and other in-band frequencies."

(d) outputting said cryptographically processed quantity to a recipient thereof.	3:18-31 – "The most elementary form of the invention is shown in FIG. 4. In data communications a hybrid 24 is sometimes used anyway. Receive channel 28 is shown extended to a receiving device, which is typically a DTMF detector at the data processing site. Very often it is necessary to transmit signals to the sending device, typically automated voice signals under the control of the data processor. For this purpose a transmit channel 30 is utilized, and hybrid 24 serves to couple transmitted signals to telephone line 26, and to couple signals on the telephone line to the receiving device over channel 28." 3:31-38 – "The hybrid serves to attenuate the transmitted signals on channel 30 such that they appear at a much lower level on the receive channel 28. As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30. Voice or even data signals may also be applied on channel 30, but the significant thing about masking signal generator 33 is that it applies a masking signal on channel 30 at the time that the sending device 10 of FIG. 1 transmits sensitive data in the opposite direction to the receiving device."

Claim 30 ('661 Patent)	**U.S. 5,181,243 to Saltwick**
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	1:34-52 – "In accordance with the principles of our invention, a masking signal is transmitted from the receiving unit during input of sensitive information at the sending device. A masking signal, as used herein, is a signal which tends to disable or confuse an eavesdropping detector. Examples are signals which distort the information signal; add to the frequency spectrum, amplitude and/or phase of the information signal; or are similar to the information signal so that a detector captures false information. The receiving unit is equipped with a means for canceling out the masking signal so that its signal detector is able to detect the information which was sent reliably and accurately. The cancellation of the masking signal is performed at the receiving site because the cancellation depends on knowledge of the specific characteristics of the masking signal and they may vary over time, e.g., in frequency, amplitude and/or phase." 3:31-33 – "As shown in FIG. 4, a masking signal generator 33 is used to apply a masking signal on channel 30." 6:6-16 – "Therefore, to keep the eavesdropping devices confused as to what the masking signal actually is, the masking signal may be varied over time in frequency, amplitude and/or phase. A random pattern is best for the receiving end to transmit. A random pattern is

	difficult for eavesdropping detectors to predict and therefore they are more likely to lose the information signal. For DTMF coding, masking signal generator 33 preferably varies the frequency between row and column frequencies, out-of-band frequencies and other in-band frequencies."
(b) improving the random characteristic of said initial noise; and	3:38-47 – "The masking signal is shown symbolically in FIG. 4, and it appears together with the information signal transmitted in the opposite direction on line 26. The function of hybrid 24 is to reduce the amplitude of the masking signal relative to that of the information signal on receive channel 28. It is in this way that the receiving device can discriminate between the information and masking signals, while an unauthorized tapping of line 26 will not result in intelligible interception of the information signal."
(c) varying said power consumption based on said improved initial noise.	5:28-52 – "The masking signal for DTMF coding can be achieved by transmitting two row frequency tones. (See FIG. 8.) A masking signal of one row frequency at the proper level would block detection of digits in the other three rows. For example, if the masking signal is the row 1 frequency (697 Hz), digits in the other three rows (2, 3, 4) would not be decoded because there would be two row tones present and this would represent an invalid DTMF signature. If the masking signal is the row 4 frequency (941 Hz), digits in rows 1, 2, 3 would not be decoded. Therefore, if two row tones are used as the masking signal, all digits will be blocked from detection. It has been found that the row 1 and row 4 frequencies are the best choices; this combination produces uniform blocking for all digits. The concept is also applicable to the use of column frequencies as masking signals. It has been found experimentally that two row frequencies and one column frequency provide the best confusion to DTMF detectors. This is primarily due to more energy at invalid frequencies being present at the decoder, thus providing greater confusion for eavesdropping detectors. (Some frequencies other than row and column frequencies have been found effective as masking signals. However, they have not thus far provided consistent masking for eavesdropping devices.)"